RSAC 2025 Conference

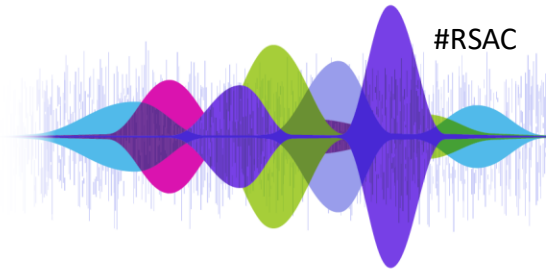
Many Voices.
One Community.

SESSION ID: IMT-T09

The Toilet Paper Principle: The Overlooked Human Side of Leading IR

Eric Olson

Director – Cyber Security
JetBlue Airways
www.linkedin.com/in/eolsondc/



Official Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

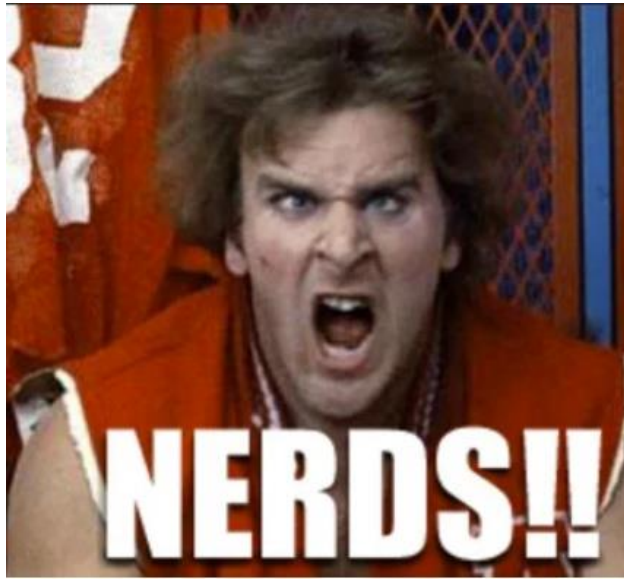
© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

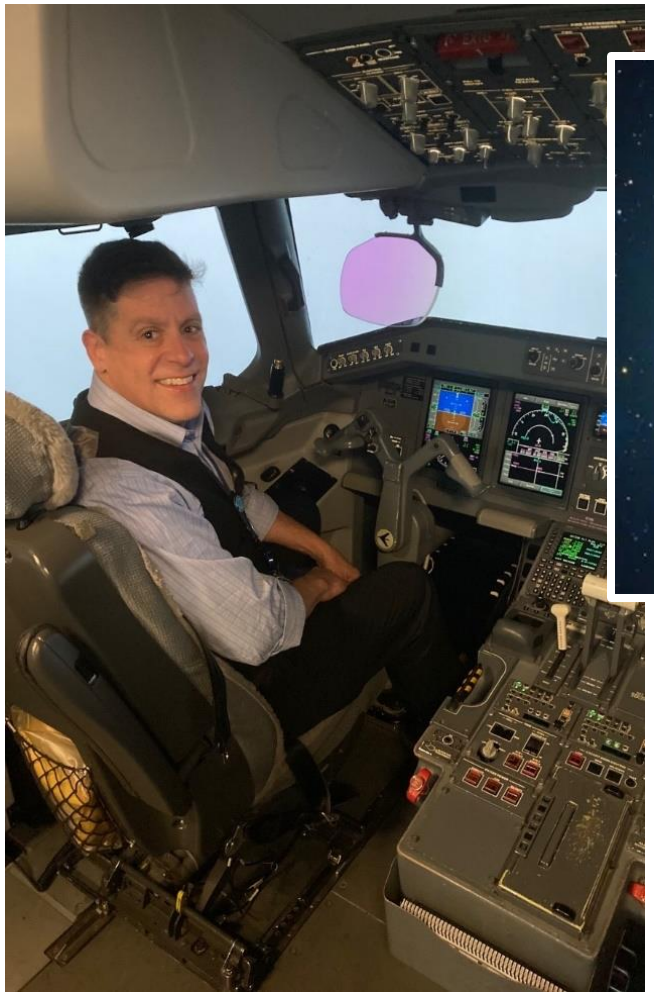
A note about taking notes

- This talk is (I hope) nearly ***all*** actionable takeaways, so…
- You can take notes but don't need to.
- RSA will make the slides available; AND
- There's a single jumplink at the end to annotated slides with takeaways on every topic.

OK, Here we go!

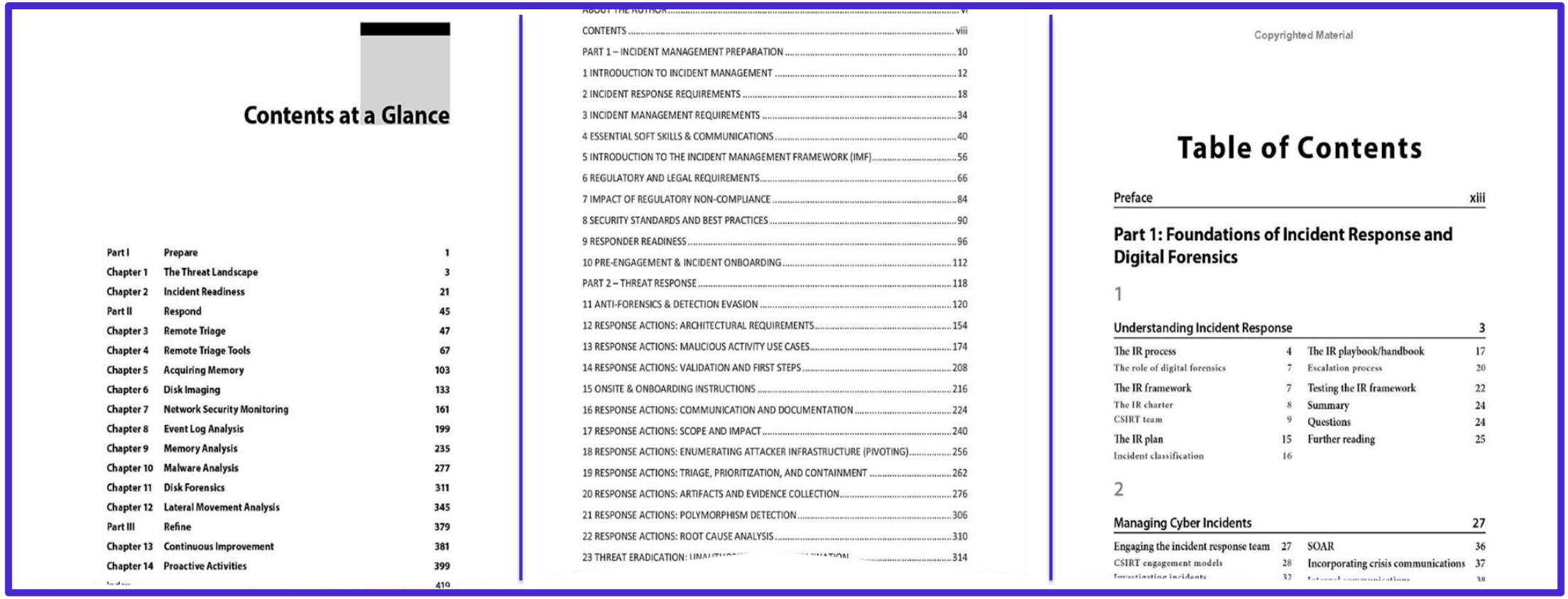
About





60-Second Origin Story

Technical Response (or "what this talk *isn't* about")



Contents at a Glance

Part I	Prepare	1
Chapter 1	The Threat Landscape	3
Chapter 2	Incident Readiness	21
Part II	Respond	45
Chapter 3	Remote Triage	47
Chapter 4	Remote Triage Tools	67
Chapter 5	Acquiring Memory	103
Chapter 6	Disk Imaging	133
Chapter 7	Network Security Monitoring	161
Chapter 8	Event Log Analysis	199
Chapter 9	Memory Analysis	235
Chapter 10	Malware Analysis	277
Chapter 11	Disk Forensics	311
Chapter 12	Lateral Movement Analysis	345
Part III	Refine	379
Chapter 13	Continuous Improvement	381
Chapter 14	Proactive Activities	399
Index		419

CONTENTS viii
PART 1 – INCIDENT MANAGEMENT PREPARATION 10
1 INTRODUCTION TO INCIDENT MANAGEMENT 12
2 INCIDENT RESPONSE REQUIREMENTS 18
3 INCIDENT MANAGEMENT REQUIREMENTS 34
4 ESSENTIAL SOFT SKILLS & COMMUNICATIONS 40
5 INTRODUCTION TO THE INCIDENT MANAGEMENT FRAMEWORK (IMF) 56
6 REGULATORY AND LEGAL REQUIREMENTS 66
7 IMPACT OF REGULATORY NON-COMPLIANCE 84
8 SECURITY STANDARDS AND BEST PRACTICES 90
9 RESPONDER READINESS 96
10 PRE-ENGAGEMENT & INCIDENT ONBOARDING 112
PART 2 – THREAT RESPONSE 118
11 ANTI-FORENSICS & DETECTION EVASION 120
12 RESPONSE ACTIONS: ARCHITECTURAL REQUIREMENTS 154
13 RESPONSE ACTIONS: MALICIOUS ACTIVITY USE CASES 174
14 RESPONSE ACTIONS: VALIDATION AND FIRST STEPS 208
15 ONSITE & ONBOARDING INSTRUCTIONS 216
16 RESPONSE ACTIONS: COMMUNICATION AND DOCUMENTATION 224
17 RESPONSE ACTIONS: SCOPE AND IMPACT 240
18 RESPONSE ACTIONS: ENUMERATING ATTACKER INFRASTRUCTURE (PIVOTING) 256
19 RESPONSE ACTIONS: TRIAGE, PRIORITIZATION, AND CONTAINMENT 262
20 RESPONSE ACTIONS: ARTIFACTS AND EVIDENCE COLLECTION 276
21 RESPONSE ACTIONS: POLYMORPHISM DETECTION 306
22 RESPONSE ACTIONS: ROOT CAUSE ANALYSIS 310
23 THREAT ERADICATION: [illegible] 314

Copyrighted Material

Table of Contents

Preface xiii

Part 1: Foundations of Incident Response and Digital Forensics

1

Understanding Incident Response 3

The IR process	4	The IR playbook/handbook	17
The role of digital forensics	7	Escalation process	20
The IR framework	7	Testing the IR framework	22
The IR charter	8	Summary	24
CSIRT team	9	Questions	24
The IR plan	15	Further reading	25
Incident classification	16		

2

Managing Cyber Incidents 27

Engaging the incident response team	27	SOAR	36
CSIRT engagement models	28	Incorporating crisis communications	37
Investigating incidents	32	Internal communications	38

The Toilet Paper Principle: What this talk *is* about

My Core Motivation? Don't Screw Up

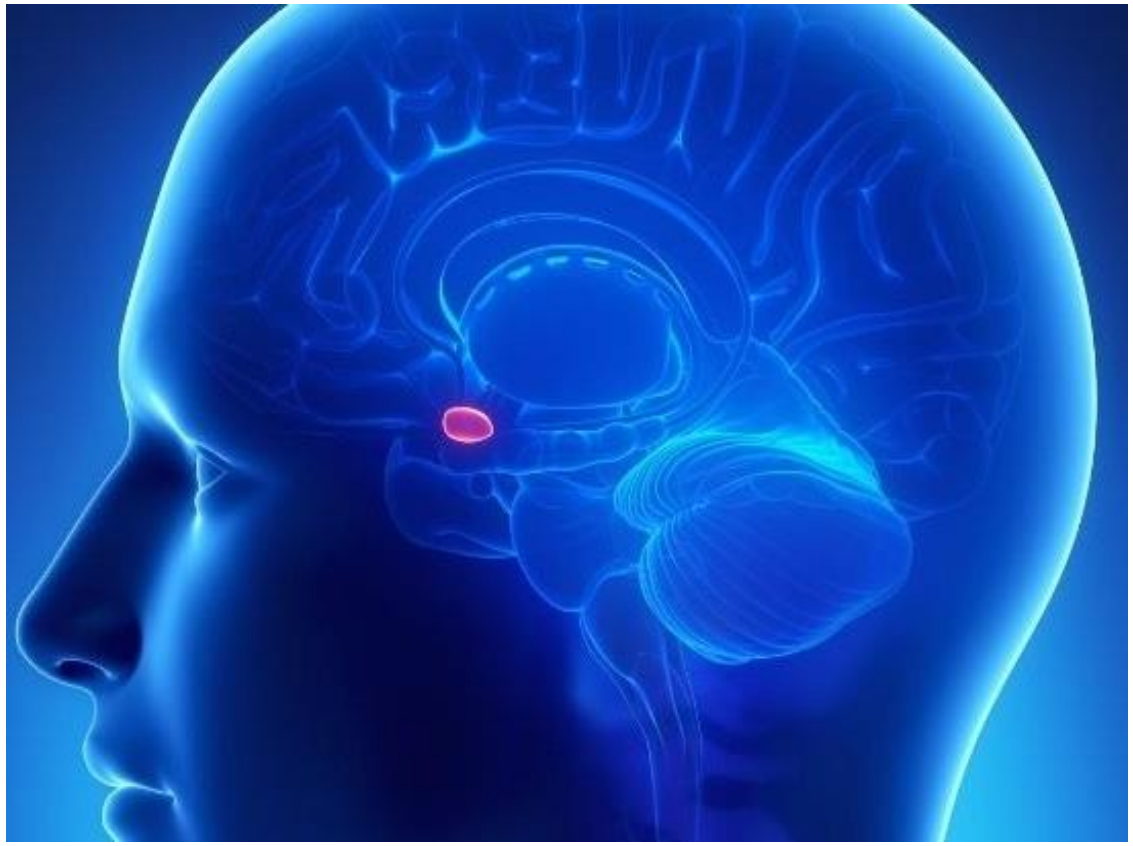
Only a fool learns from his own mistakes. The wise man learns from the mistakes of others.

~ Otto von Bismarck

My “Research” Methodology

Before the storm

Here's one that's not in the manual



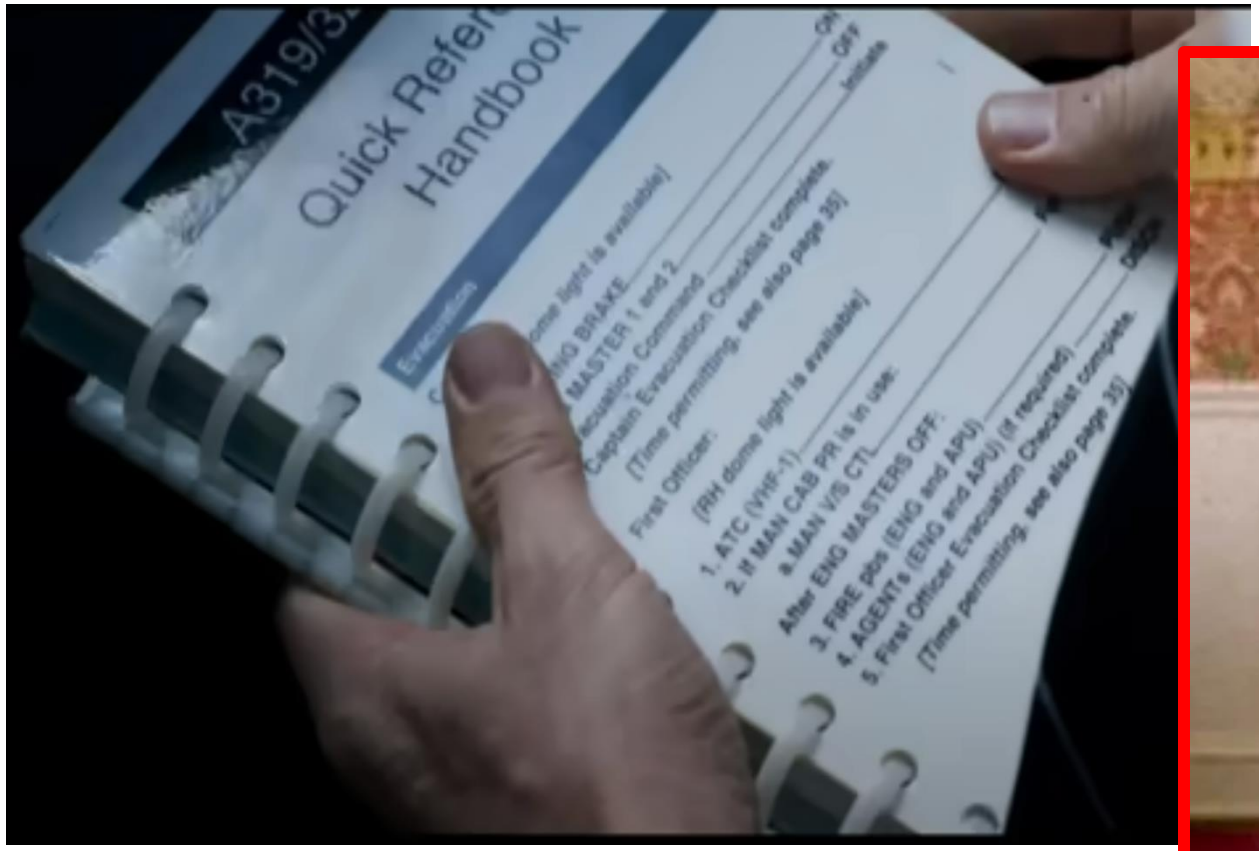
"Stress is not a state of mind... it's a condition that reduces the ability of your brain to function properly." **- Gabor Mate**

Everything else starts from this

"In high stress situations, people don't rise to the occasion, they sink to the level of their training."

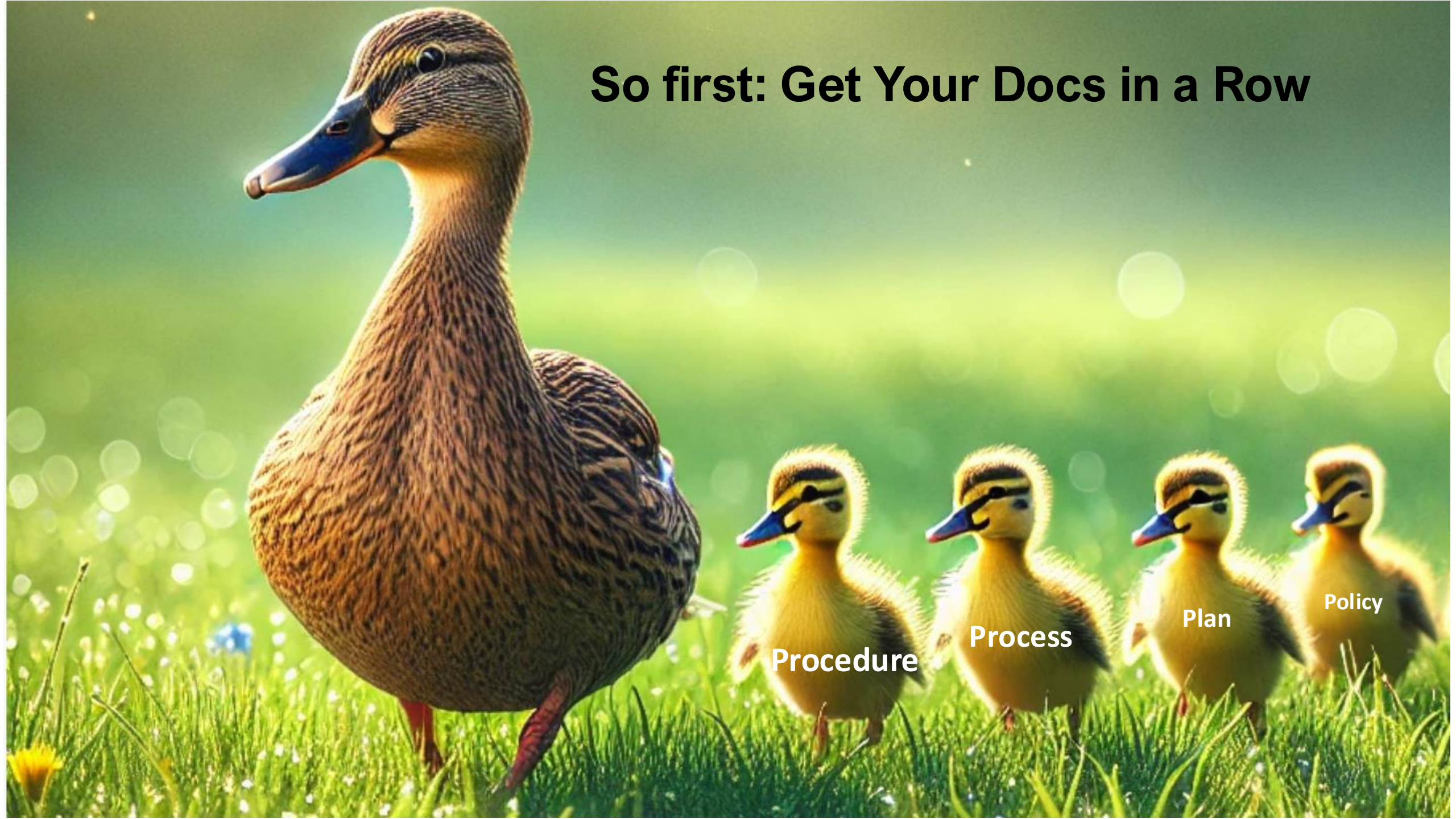
- *Nick S.*
  - *IR Company CEO*
  - *Former CISO*
  - *IFR Pilot*
  - *Working Detective*

In other words…


Quick Refer
Handbook
A319/3
Evacuation
Captain Evacuation Command
(Time permitting, see also page 35)
First Officer:
[RH dome light is available]
1. ATC (VHF-1)
2. If MAN CAB PR is in use:
a. MAN V/S CTL
After ENG MASTERS OFF:
3. FIRE pbs (ENG and APU)
4. AGENTs (ENG and APU) (if required)
5. First Officer Evacuation Checklist complete
(Time permitting, see also page 35)

Without this ^^

We all turn into this ==>


So first: Get Your Docs in a Row
Procedure
Process
Plan
Policy

How to think about an IR *Policy*

Good things. Do:

- Keep it short. (Nope. Shorter than that.)
- Document the organization's commitment to detecting & responding to cyber Incidents.
- Define high-level roles by title or department.
- Explicitly assign authority & accountability.
- Specify regulatory & compliance req's such as PCI that the IR function should align to.
- Use it to allow budgeting and drive behavior.
- Not much else.

Not-so-good things. Don't:

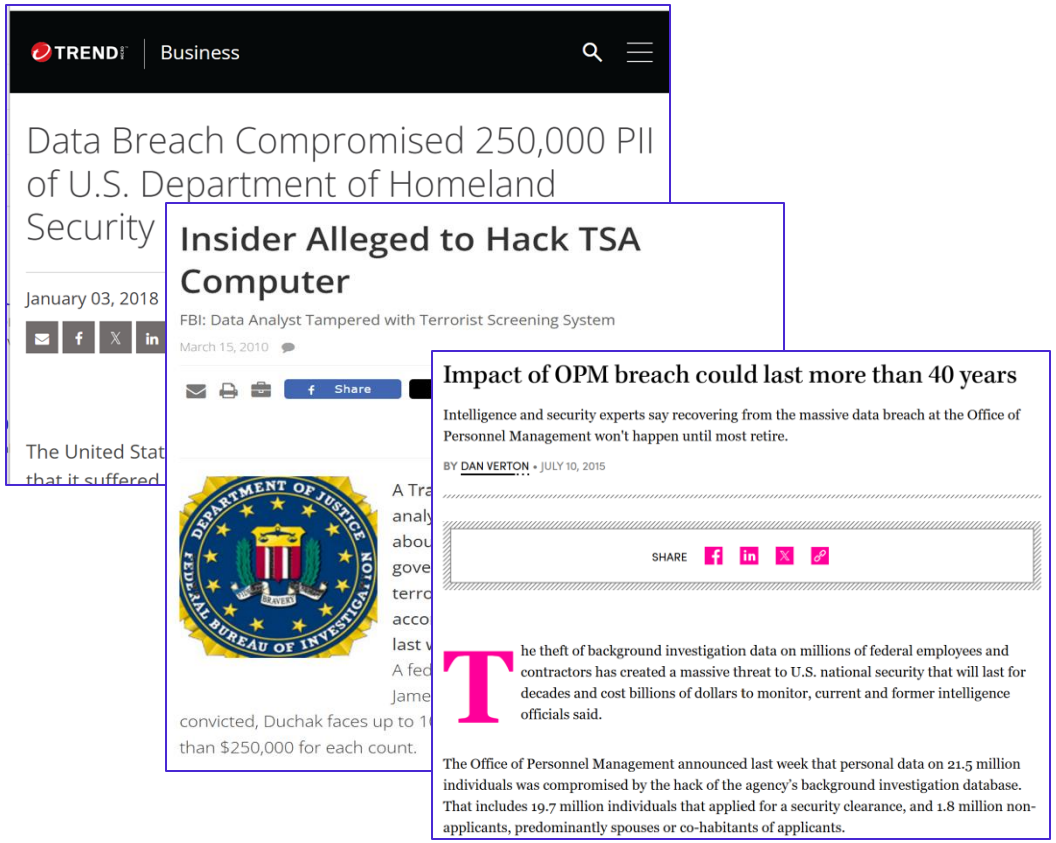
- Explain *how* the organization will respond to cyber Incidents.
- Identify *who* is responsible by name instead of department, function or title.
- Name any specific tools, systems or controls
- Specify processes, procedures, playbooks or anything at an actionable level of detail.

Rule of thumb? If it contains names of people, vendors, systems or any kind of process, it's in the wrong document.

Why keep *Policy* docs short and generic?

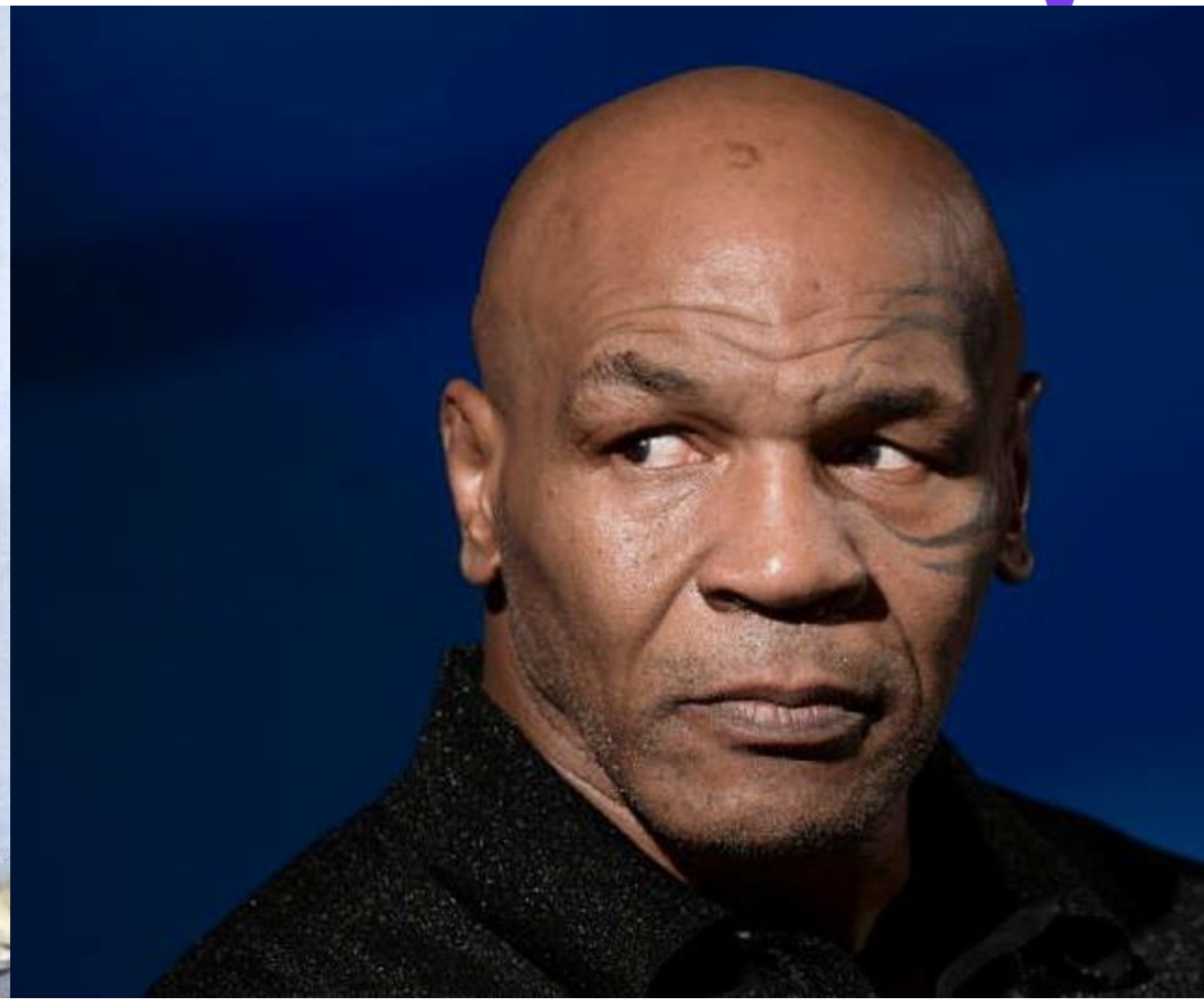
Giving detail to oversight bodies is a *terrible* idea.

- Living documents are constantly updated, *submitted* docs need to be generic to minimize churn and effort.
- Regulators often suck at security, do *not* give give them your defensive blueprint to lose.
- If discovered, attacks will target your implied weaknesses and existing processes.
- Named individuals *will* be researched, targeted and phished.


TREND
Business
Data Breach Compromised 250,000 PII of U.S. Department of Homeland Security
January 03, 2018
Insider Alleged to Hack TSA Computer
FBI: Data Analyst Tampered with Terrorist Screening System
March 15, 2010
Share
Impact of OPM breach could last more than 40 years
Intelligence and security experts say recovering from the massive data breach at the Office of Personnel Management won't happen until most retire.
BY DAN VERTON • JULY 10, 2015
SHARE
The theft of background investigation data on millions of federal employees and contractors has created a massive threat to U.S. national security that will last for decades and cost billions of dollars to monitor, current and former intelligence officials said.
The Office of Personnel Management announced last week that personal data on 21.5 million individuals was compromised by the hack of the agency's background investigation database. That includes 19.7 million individuals that applied for a security clearance, and 1.8 million non-applicants, predominantly spouses or co-habitants of applicants.
than $250,000 for each count.

On the importance of a Plan

On the other hand, on the limits of a Plan



IR *Plan* do's and don'ts

A good Plan document:

- Applies equally well to most types of incident
- Defines terminology around cases, incidents, severity, criticality etc.
- Labels phases of an Incident based on your choice of model
- Articulates escalation paths and requirements
- Addresses roles & responsibilities, division of duties, use of outside partners or counsel and retainer invocation criteria & authority

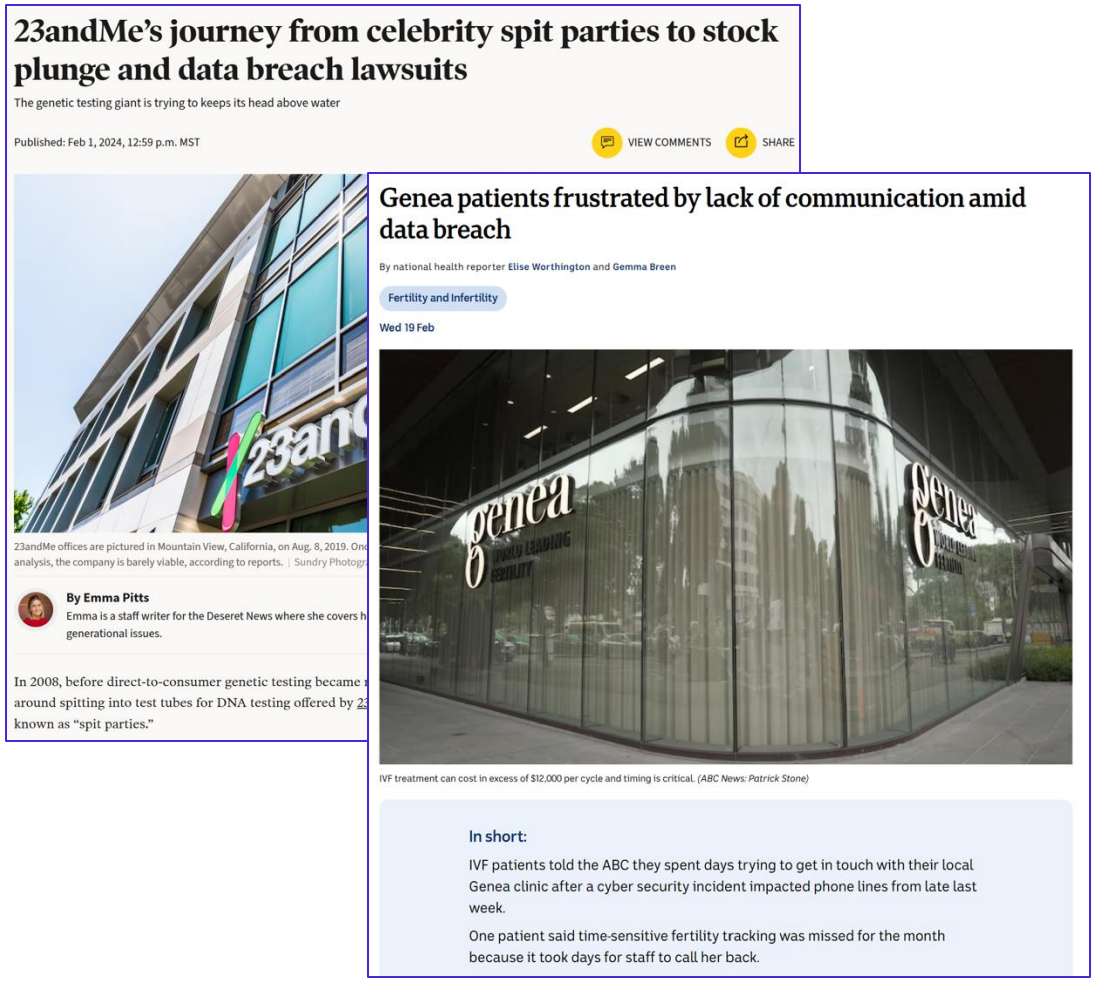
It still doesn't:

- Define processes or name tools or vendors
- Name individuals inside the organization or at partners and providers
- Describe in-place controls
- Discuss/reveal how containment would be accomplished for specific cases
- Require constant revision based on continuous improvement and learnings from each incident

What happens when you don't do it well

It always matters, but…

- Trust-based businesses are especially vulnerable to poor IR planning or response
- Ex: Genea IVF lost 700GB of customer data
- They waited a week to tell anyone, and then made a hash of the response
- 23andme paid $30m after failing completely to secure the *most* personal data there is
- Due to a mix of the breach and other factors, 23andme's value fell… ***98%***



23andMe's journey from celebrity spit parties to stock plunge and data breach lawsuits

The genetic testing giant is trying to keeps its head above water

Published: Feb 1, 2024, 12:59 p.m. MST

VIEW COMMENTS SHARE

23andMe offices are pictured in Mountain View, California, on Aug. 8, 2019. On analysis, the company is barely viable, according to reports. | Sundry Photogr

By Emma Pitts

Emma is a staff writer for the Deseret News where she covers h generational issues.

In 2008, before direct-to-consumer genetic testing became around spitting into test tubes for DNA testing offered by 23 known as "spit parties."

Genea patients frustrated by lack of communication amid data breach

By national health reporter Elise Worthington and Gemma Breen

Fertility and Infertility

Wed 19 Feb

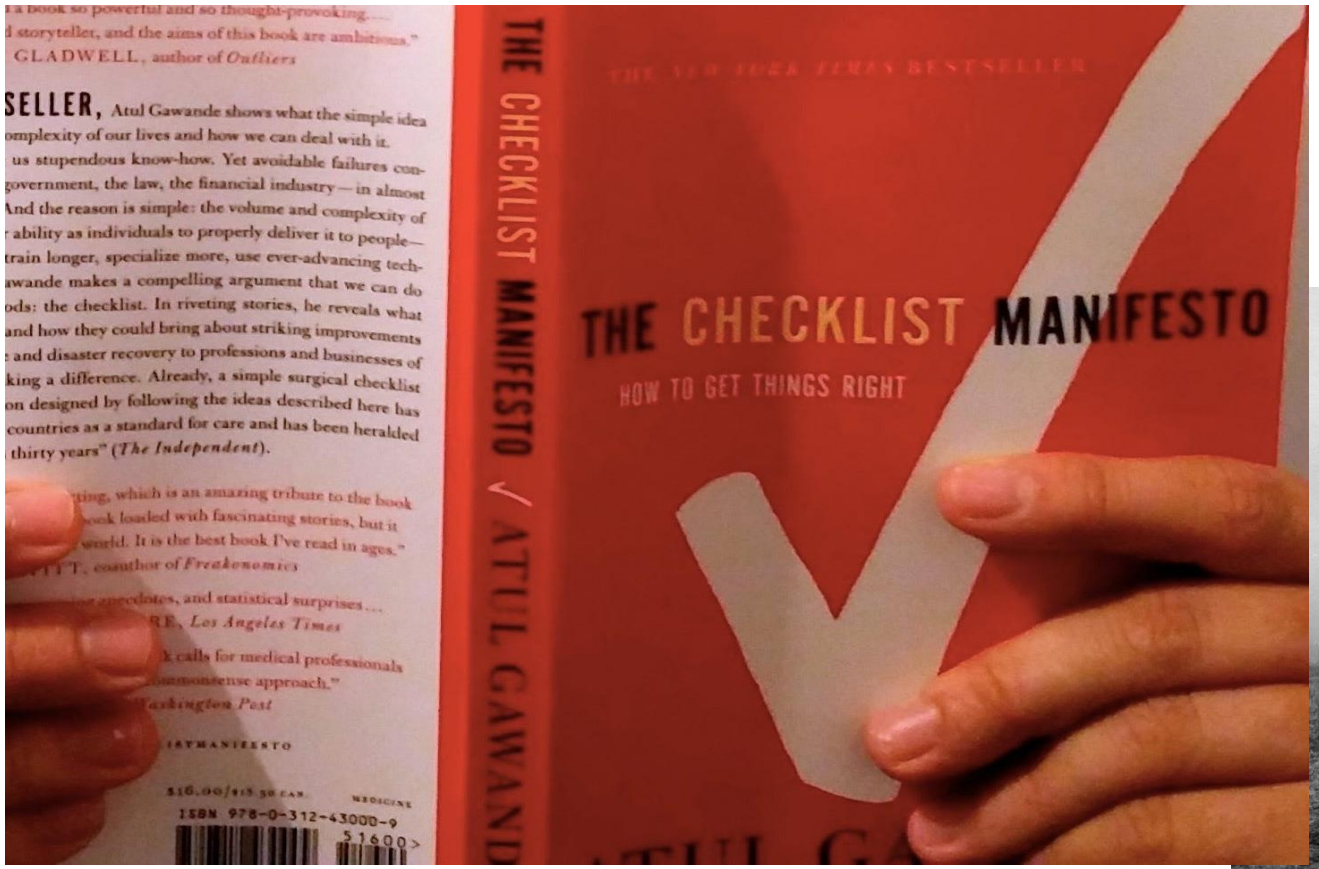
IVF treatment can cost in excess of $12,000 per cycle and timing is critical. *(ABC News: Patrick Stone)*

In short:

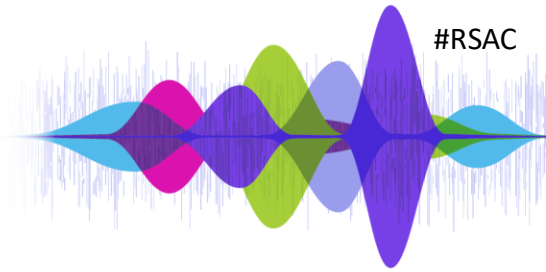
IVF patients told the ABC they spent days trying to get in touch with their local Genea clinic after a cyber security incident impacted phone lines from late last week.

One patient said time-sensitive fertility tracking was missed for the month because it took days for staff to call her back.

It’s not just the Plan, it’s the Procedures



Processes Vs. Procedures



Process Documents:

- For people who actually respond to Incidents
- Provide structured workflows, and a specified series of steps
- Differ for different types of Incidents.
- Standardizes the sequence of key tasks for each type to ensure consistent handling.
- It still does not dictate *tool-specific* instructions or individual mouse clicks.

Procedures:

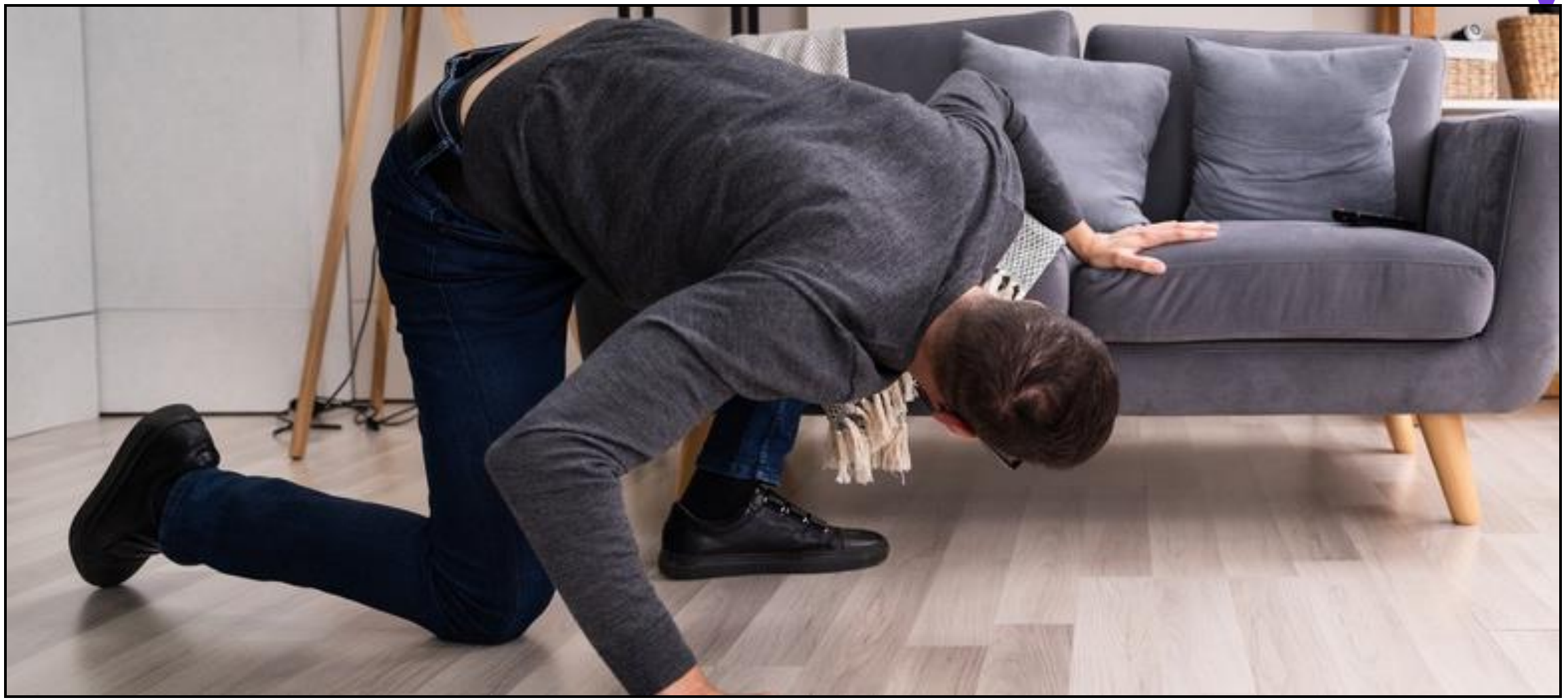
- This is the most granular level. Its purpose is step-by-step instructions for dealing with a specific type of case.
- This *does* spell out tool-specific system commands, menus and UI navigation.
- Think of Procedures as follows:
  - “Oh, you’re the new guy?”
  - “OK, when we say ‘isolate that host via the EDR console’ we mean do this. Exactly this.”
  - “Follow the the screenshots on page 3.”

Current Procedures, in Binders!

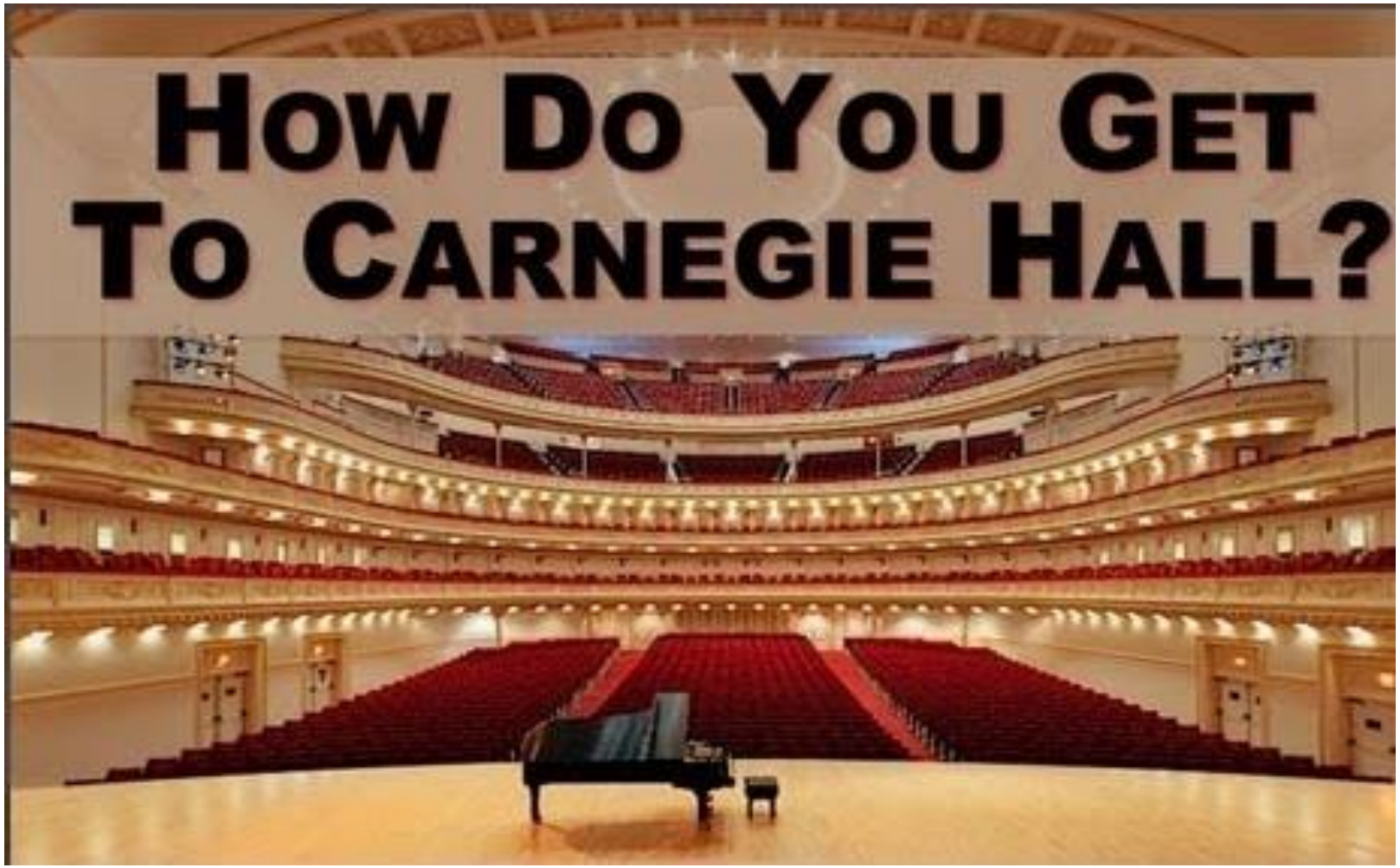
The List by the Phone

The Smokejumpers

Now where did you put your (API) keys?



Don’t count on what you don’t test



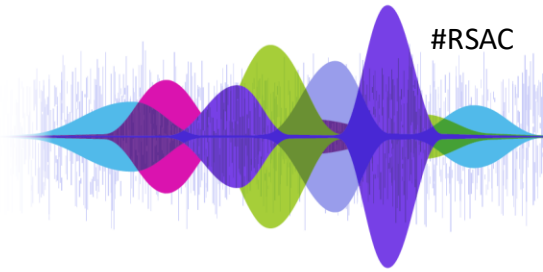
- Regular tabletops
- Single-process drills
- Attack Sims
- Purple Team Exercises
- Control Validation Scripts
- ***Consistency over breadth***

Play the B team

Remember your emergency comms*

** are discoverable*

Summary: Before the bad day comes



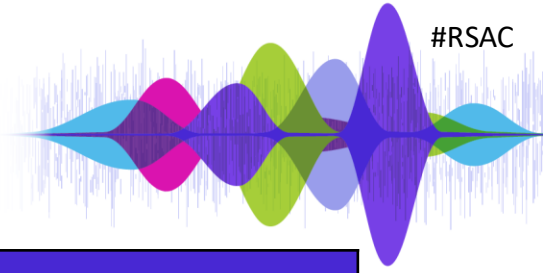
- Understand the importance of docs at different levels & for distinct audiences.
- Brains in freakout mode don't improvise well. Don't expect or need them to.
- Policy serves to address the authorities and the auditors, *not* the Responders.
- Create Plans that explain roles, duties, escalations and stages of incidents.
- Draft Processes and Procedures that empower people who do actual work to do it right, even if it's their first day on the job.
- Make sure everyone knows who to inform *and* who to call for help, how to reach them, what access they need, and who rings the panic bell.
- Assume compromise and/or loss of your comms, your plans and your docs; have backup facilities, and keep all critical information *on paper*.
- Then practice. Then add curveballs and practice some more. Then again.

The Day Arrives…

The First Question – Who's In Charge?

The Incident Commander

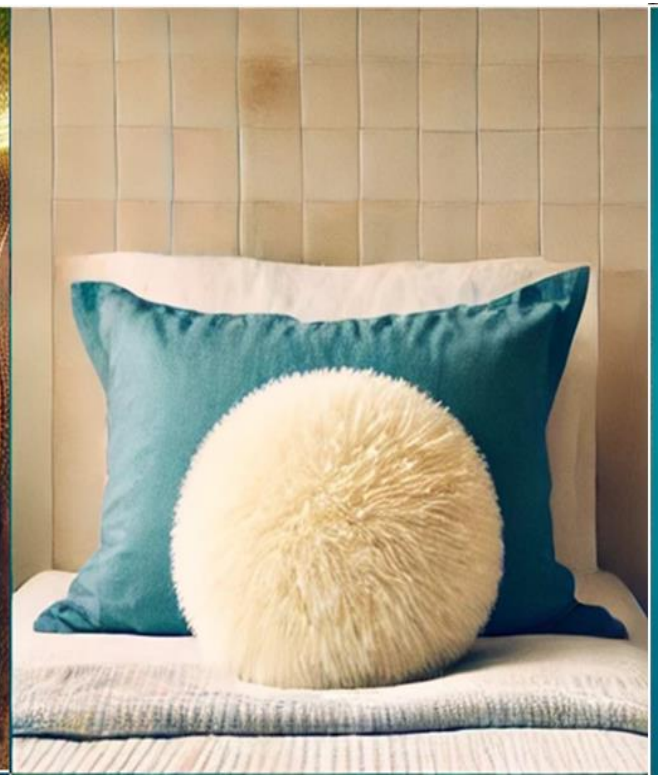
Clear authorities avoid confusion & delay



EXAMPLE MATRIX: Decision Type	Commander 's Role & Authority	Business Leaders' Role & Authority
Tactical Security Response (e.g., isolating compromised systems, blocking network traffic)	Incident Commander has full authority, within pre-defined IR playbooks	Not Applicable, as the IC is empowered to execute autonomously
Forensic and Technical Investigations	Determines scope and methodology	Can offer guidance, surface any constraints, but does not dictate
Containment & Remediation Actions	Full authority unless the action has the potential for material business impact *(May benefit from an actual $/$$/$$$ matrix)*	Leadership must authorize if decisions will materially impact customers, operations, revenue or shareholders
Customer, Media and Regulatory Communications	Provides factual input, technical support, but does not speak to any outside parties unless requested	Legal, PR, Crisis Comms and/or SLT own and control press, customer and/or regulatiory disclosures and messaging
Financial and Legal Risk Assessment and Decision-Making	Serves as advisor and consultant, providing technical assessment and insights into possible business risk or impact analysis	SLT (GC, CEO, CFO) own all decision-making
Incident Closure and Lessons Learned	Leads technical review and documentation, reports summary to ELT, Board or others *as directed*	Business leadership integrates insights, improvements and key learnings into evolving Enterprise Risk Strategy

ASAP: Try to Understand the race you’re in

Care & Feeding



Nuthin’ happens without money…

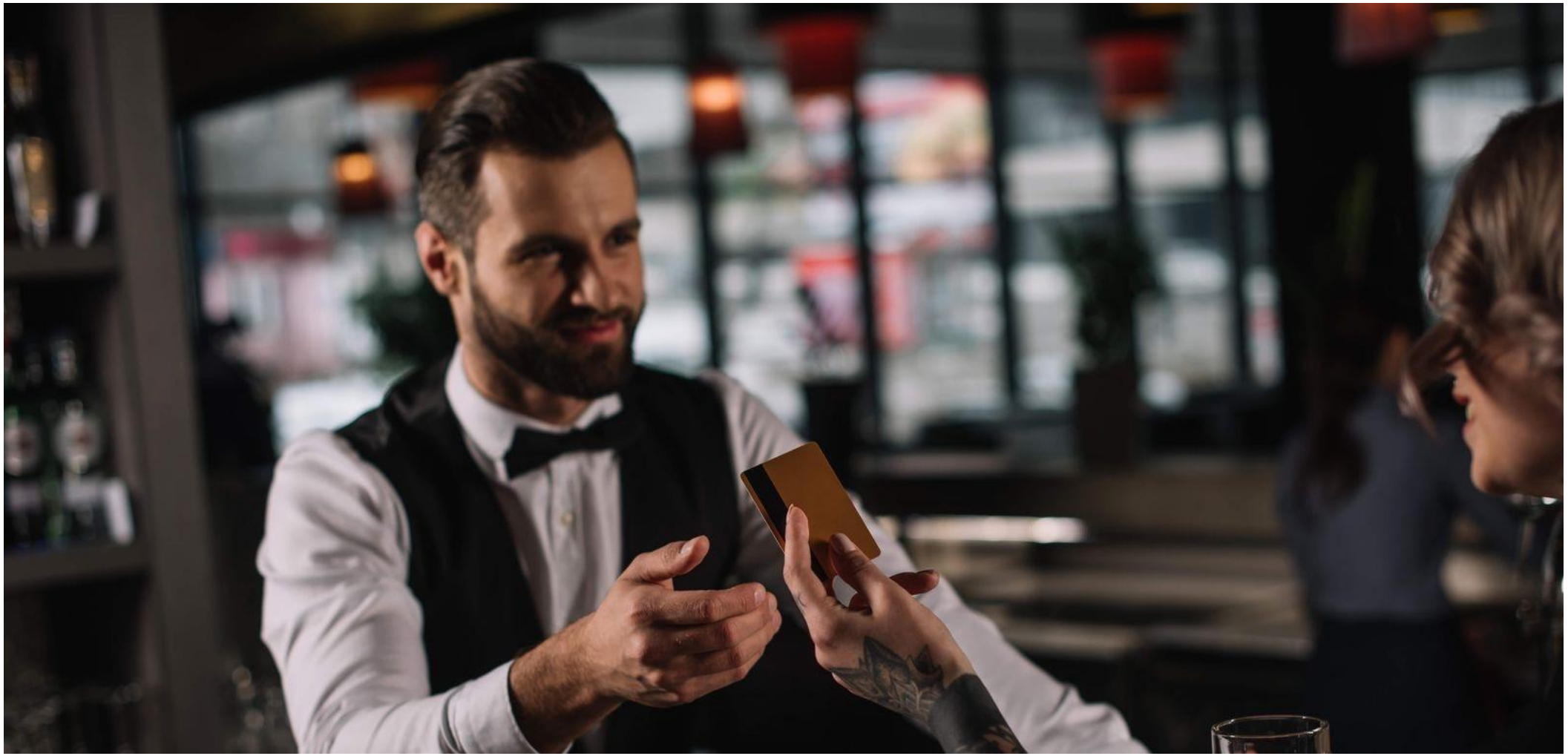
Immediately unleash both people resources to get your heroes what they need.

Get off the phone!

Anyone who you don't need *on* the phone should get *off* the phone!

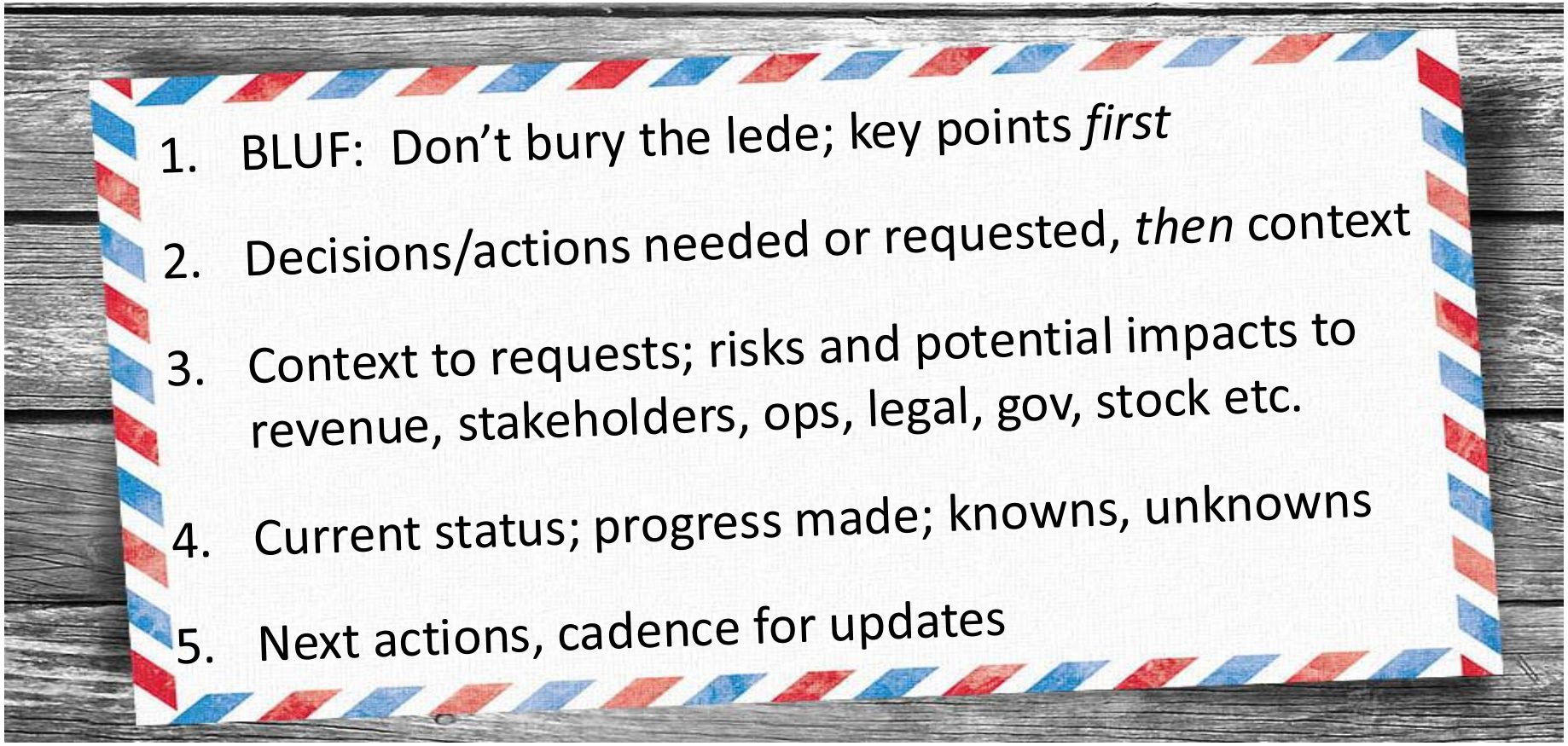
1. Day Jobs and BAU – Anyone on the hotline isn't keeping the trains running
2. Division of Labor – If you have scarce key skills, some need to rest while others work
3. Bloodsucking leeches – Contractors and consultants get paid whether they contribute or not
4. Leaky buildings – Anyone who doesn't *need* to know, *shouldn't* know

Keep your tab open



Write it down. (Very, very carefully.)

Postcards to Leadership


1. BLUF: Don't bury the lede; key points *first*
2. Decisions/actions needed or requested, *then* context
3. Context to requests; risks and potential impacts to revenue, stakeholders, ops, legal, gov, stock etc.
4. Current status; progress made; knowns, unknowns
5. Next actions, cadence for updates

The reply to expect:

Hey Nerds!

1. **What's up?**
2. **How bad is it?**
3. **Whatcha doing?**
4. **When RTO?**

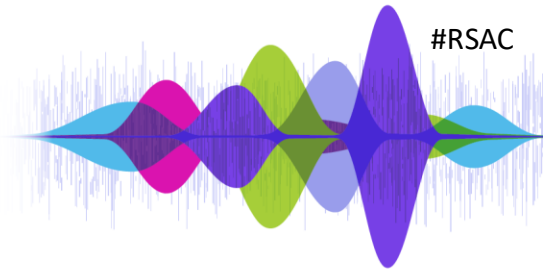
Do: Make updates short, factual, regular. ***Do Not***: Include feelings, speculation, debate, geek speak. ***Do not*** get into fault or I-told-you-so's. RCA is for later. **For now, don't fix the blame, fix the problem.**

The changing of the guard

Good and bad help

#RSAC
RSAC 2025 Conference

Summary: In the heat of the fight



- Be crystal clear on what decisions sit where, and who's in charge of what
- Try to assess what kind of race you're in, and respond accordingly regarding shifts, resources, single PoFs, staff and retainer partners
- If it's a marathon, *immediately* assign resources to take care of human needs; don't wait til your people are already frayed and exhausted to care for them
- Create, or activate, the vehicle to pay for what is needed, get it, and track it
- Document, and communicate, effectively; quality comms are consistent, informative, and request any needs or decisions clearly
- They also presume eventual discovery, litigation and second-guessing by Monday-morning quarterbacks, so they are judicious, factual and brief
- Identify and enlist good help, deny and resist "bad help"

The Storm Has Passed

The AAR

AFTER ACTION REVIEW
WHAT HAPPENED?
WHY IT HAPPENED?
HOW TO DO BETTER?

Relentlessly pursue due-outs to closure

Down time

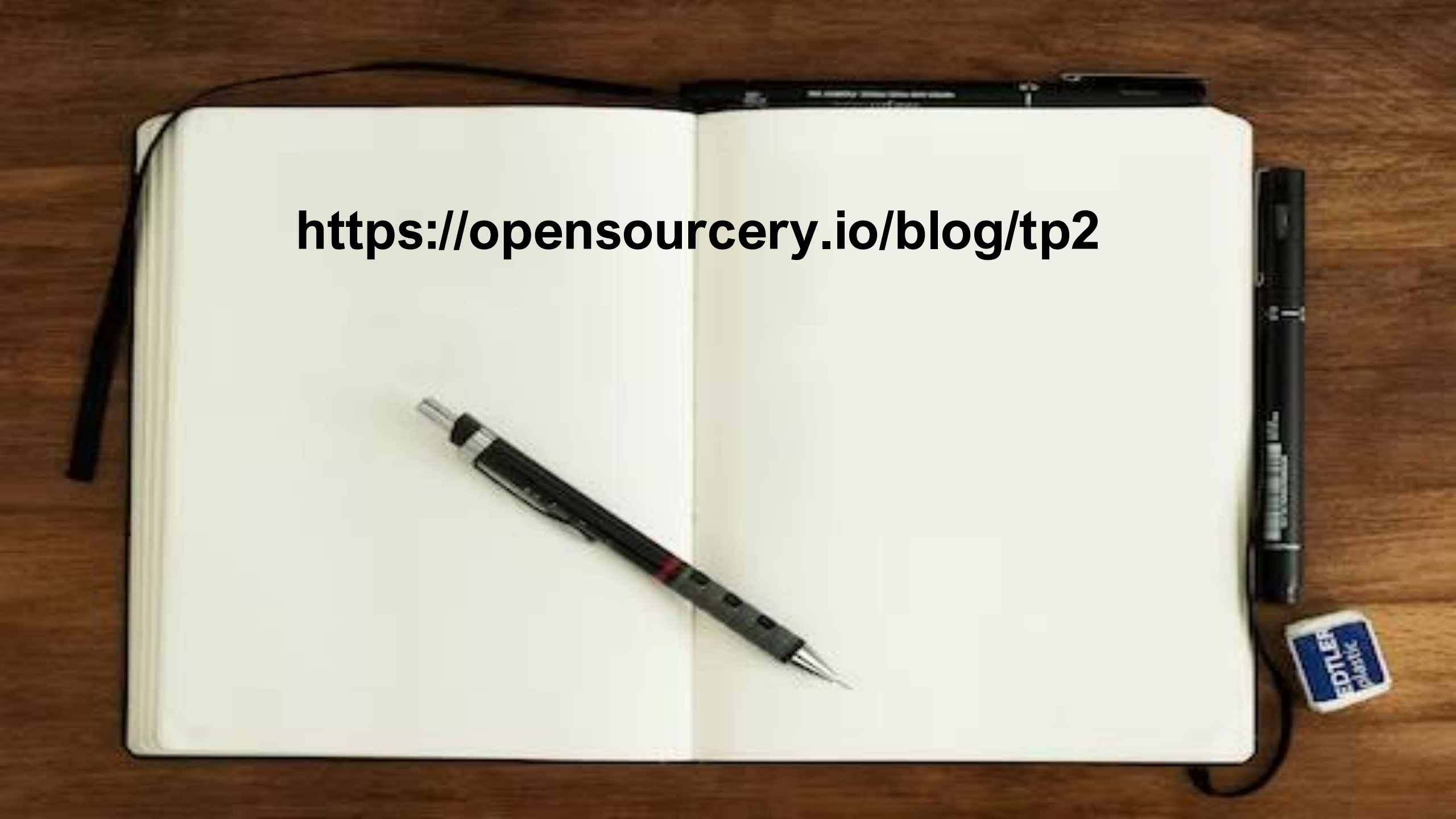
#RSAC
RSAC 2025 Conference

But… cover your asse(t)s

In closing then…

- This is a very human business, and humans need to be not just managed but cared for.
- Incident Preparation is better, cheaper and *less stressful* than Incident Response.
- The more you do, organize and document *before* you need it;
- The more you *plan* for the long-haul and take care of people while that marathon is going on;
- The more you practice before the bad day comes; and
- The better you capture, run down and *learn from* each Incident
- The better you do that, the better you get and the less it hurts next time.

https://opensourcery.io/blog/tp2



Q & A

RSAC 2025 Conference

Many Voices.
One Community.

Connect, ask questions, PDF of slides etc.

Eric@polestar.llc

linkedin.com/in/eolsondc/